Notice of Allowability	**Application No.** 10/815,572	**Applicant(s)** MIRONOV ET AL.
	Examiner JOSEPH PAN	**Art Unit** 2435

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *8/29/08*.

2. ☒ The allowed claim(s) is/are *1-40*.

3. □ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) □ All b) □ Some* c) □ None of the:
   1. □ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. _____ .
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
   1) □ hereto or 2) □ to Paper No./Mail Date _____.
   (b) □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. □ Notice of References Cited (PTO-892)
2. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. □ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *here with* .
7. ☒ Examiner's Amendment/Comment
8. □ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

DETAILED ACTION

1. An examiner's amendment to the record appears below. Should the changes and/ or additions be unacceptable to Applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

2. Authorization for this examiner's amendment was given in a telephone interview with Mr. Dominic S. Lindauer, of registration number 61,417, on December 1, 2008. During the telephone conference, Mr. Lindauer has agreed and authorized the examiner to amend Claims 31-40.

CLAIMS

3. Replacing Claims 31-40 as following:

a. Claim 31:

One or more computer storage media having instructions stored thereon that, when executed, direct a machine to perform acts comprising:

strengthening an existing stream cipher's output by sequentially storing pointers to a plurality of results provided by the stream cipher in a first, second, and third storage units;

providing a plurality of results from a pairing function, the pairing function pairing individual values from the first and third storage units that are at least a threshold value apart, wherein the pairing function is $p(x,y) = x \oplus (ay+b)$, where *a* and *b* are two constants, and *a* is odd or $p(x,y) = \gamma, \delta$ is chosen as a nearly universal hash function by the iteration of the following rules:

$$\alpha = ax \bmod 2^{2n}$$

$$\beta = by \bmod 2^{2n}$$

$$\gamma = \alpha^{L} + \beta^{R} \bmod 2^{2n}$$

$$\delta = \alpha^{R} + \beta^{L} \bmod 2^{2n},$$

where x^L and x^R respectively denote left and right halves of *x*, and *a,b* are chosen randomly;

upon reaching the threshold value of the existing stream cipher output, serially and recursively rotating contents of the first, second, and third storage units, thereby strengthening the cipher stream, wherein the contents of the storage units are the pointers; and

outputting the now strengthened stream cipher.

b. Claim 32:

One or more computer storage media as recited by claim 31, wherein a short-term correlation between the individual values from the first and third storage units is limited.

c. Claim 33:

One or more computer storage media as recited by claim 31, wherein a length of each of the first, second, and third storage units equals the threshold value.

d. Claim 34:

One or more computer storage media as recited by claim 31, wherein the first, second, and third storage units are implemented in a single memory device.

e. Claim 35:

One or more computer storage media as recited by claim 31, wherein the serial rotation is performed by shifting the first, second, and third storage units in a same direction.

f. Claim 36:

One or more computer storage media as recited by claim 31, wherein the pairing function results are stored in a table.

g. Claim 37:

One or more computer storage media as recited by claim 31, wherein the acts are performed recursively.

h. Claim 38:

One or more computer storage media as recited by claim 31, wherein the existing stream cipher is combined with one or more update rules selected from a group comprising random walks, T-functions, LFSRs (linear feedback shift registers), and word-based stream ciphers.

i. Claim 39:

One or more computer storage media as recited by claim 38, wherein the random walks are selected from one or more walks in a group comprising an additive walk, a multiplicative walk, a Gabber-Galil walk, a Ramanujan walk, a permutation walk, and a random walk with a dynamic generator.

j. Claim 40:

One or more computer storage media as recited by claim 31, further comprising enhancing the pairing function by utilizing a fourth storage unit.

ALLOWABLE SUBJECT MATTER

4. Claims 1-40 are allowed.

CONCLUSION

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-6300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/Joseph Pan/
Examiner, Art Unit 2435
December 2, 2008
/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435